Sirbi i Protehá
PRO JUSTITIA
KORPS POLITIE CURACAO

Proces-verbaal van Aangifte

Proces-verbaalnummer	:	202602261200.AANG
Documentcode	:	

Naam Verbalisant	:	A.Bhattoe werkzaam binnen het Korps Politie Curaçao, ingedeeld bij Team Zwacri 2
Art. + omschrijving	:	Van het Wetboek van Strafrecht Curaçao, Uitvoering Voltooid Feit: • 2:69 (Hacking) Lid 1 Sub A 2:289 (Diefstal) Sub B • 2:404 t/m 2:406 (Witwassen) • 2.305 (Oplichting) • 2:184 (Valsheid ingeschrifte) • 2:308 (misbruik maken van telecommunicatiedienst)
Gepleegd op/tussen	:	Sunday 11 januari 2026 omstreeks 06:22 AM,
PD	:	lease server Germany and Netherlands
Datum /tijd / plaats aangifte	:	Donderdag 26 februari 2026 om 12:00 te Politie Bureau Rio Canario
		UBO
Achternaam	:	Aktolkyn Zhetkervenova
Geboortedatum	:	29.09.1993
Geboorteplaats	:	Shymkent,Kazakhstan
Woonpl. + adres	:	St. E-36, Building 4, apt., 498, Astana
Beroep	:	company UBO
Nationaliteit	:	Kazakh
Identiteit conform	:	Paspoort
Telefoonnummer	:	+79178803706
Email	:	limescoltd@gmail.com

Achternaam	:	Gouloud
Voornamen	:	Mecedes Hammoud

Geboortedatum	:	**11 maart 1962**
Geboorteplaats	:	**Curacao**
Woonpl. + adres	:	**Kaya Richard J. Beaujon Z/N Landhuis Joonchi II**
Beroep	:	**Directeur van G-Force Corporate Services B.V. / Guardian Corporation Curaçao B.V**
Nationaliteit	:	**Nederlands**
Telefoonnummer	:	**+59996995543**
Email	:	**gouloud@gfcgroup.co**

Verklaring Aangever:
☒**Gouloud, Mecedes Hammoud**, legde een verklaring in het Engelse taal af, welk door mij, verbalisant, in het Enegels op schrift werd gesteld en als volgt luidde:
☒Ik, verbalisant, ben het machtig in woord en/of geschrift.

WoT N.V. hereby formally submits a criminal complaint to the Korps Politie Curaçao regarding a serious cybercrime incident that occurred on **11 January 2026 at 06:22 AM**, resulting in the unauthorized withdrawal and subsequent laundering of cryptocurrency assets through fraudulent API activity on the company's payment server.

WoT N.V. — Company Explanation

Type of company
WoT N.V. is a Curaçao offshore entity. It operates under the legal framework for offshore companies established in Curaçao. De staturory director of this company is G-Force Corporate Services B.V. / Guardian Corporation Curaçao B.V.

Services provided
WoT N.V. is an online e-gaming provider licensed by the Curaçao Gaming Authority (CGA). This means the company is authorized to operate online gaming platforms, process player transactions, and provide digital gaming services under Curaçao's regulatory regime.

Server location
The operational servers of WoT N.V. are hosted in Germany and The Netherlands, specifically in Leaseweb data centers. These servers include the payment processing server that was compromised.

Incident Summary (as confirmed by WoT N.V.)

On 11 January 2026, an attacker gained unauthorized access to WoT N.V.'s payment processing server, hosted at Leaseweb datacenters in Germany and the Netherlands. The attacker obtained API keys used to communicate with the cryptocurrency payment provider Alphapo.

Using these stolen API keys, the attacker initiated fraudulent withdrawal requests, which Alphapo processed as legitimate. The stolen funds were then transferred to blockchain wallets controlled by the attacker and subsequently moved to exchanges including HitBTC ; CoinEx and the USDC issuer Circle consistent with money laundering behavior.

As a result of this intrusion:

- data was deleted,
- critical services were disabled,
- system integrity was compromised, and
- sensitive API credentials were exposed.

During the same timeframe, digital assets (USDC, USDT, BTC) were withdrawn without authorization via compromised API access to the third-party payment provider Alphapo.

These withdrawals:

- were not initiated by WoT N.V.,
- were not approved by any authorized personnel,
- were executed programmatically, not via wallet login,
- were authenticated using stolen API credentials, and
- were processed as valid by Alphapo's system.

Clarification: No Wallet Login or Private Key Theft WoT N.V. confirms:

- No blockchain wallet was accessed directly.
- No private keys were compromised.
- No 2FA or wallet authentication was bypassed.
- No wallet interface was used.

All unauthorized withdrawals occurred via Alphapo's API, using credentials stolen from the compromised server.

Therefore:

- Wallet-level logs,
- IP addresses used for withdrawal execution,
- Device fingerprints,
- Authentication logs

are only available from Alphapo, not from WoT N.V.

What are API Keys?
API keys are digital access credentials that allow secure communication between two systems. In this case, WoT N.V.'s payment server used API keys to authenticate with Alphapo, enabling:

- legitimate withdrawal requests
- balance checks
- transaction processing

An API key functions like a digital signature:

- Any request signed with this key is treated as authorized by the payment provider.

How the attacker misused the API keys

According to the investigation:

- The attacker gained unauthorized access to WoT N.V.'s payment server.
- The attacker extracted the API keys stored on the server.
- Using these keys, the attacker sent fraudulent withdrawal commands to Alphapo.
- Alphapo's system accepted these commands as legitimate because the API keys were valid.
- Funds were transferred to attacker-controlled wallets.

Logs and Technical Evidence

Logs available from WoT N.V.:

- server access logs,
- infrastructure logs,
- application/API request logs,
- evidence of unauthorized server access.

Logs NOT available from WoT N.V.:

- wallet login logs,
- IP addresses used for withdrawal execution,
- device fingerprints,
- authentication logs.

These are held exclusively by Alphapo.

Internal IT & Security Team of WoT N.V.
They analyzed:

- server logs
- API request logs
- payment system records
- access patterns
- timestamps of unauthorized withdrawals

Alphapo's Investigation Team
They performed:

- blockchain tracing
- hop-by-hop fund movement analysis
- tagging of stolen funds in Chainalysis & Crystal Blockchain
- identification of exchanges involved (Circle, HitBTC, CoinEx)

Stolen Cryptocurrency Assets

USDC

- 65,498.50453 USDC
- 1,853.839505 USDC

Allocated at:
0x9059Ab4C07d3bB0fC5a4E1B28271F7c44b9b4075

USDT (TRC-20)

- 19,438.88959234 USDT
- 333.92 USDT

Allocated at:
TP6q7hHnF9uWpsAXJBHci6j6XNHeoHWBGp
BTC

- **0.14328483 BTC**

Allocated at:
bc1qt6s78vfjrxxuueqq843smu0sk8m25j0yp7zsac

Movement of Stolen Funds

- Funds were traced hop-by-hop using Chainalysis and Crystal Blockchain.
- Part of the funds reached HitBTC.
- Later, funds were moved to CoinEx (confirmed by transaction hash 0xe5743e475260c093ac31f6a536c867dfc41628e649cd7223c21caaff8c7f0398).
- Stolen transactions have been marked as 100% Fraud in blockchain intelligence systems.
- **Circle** is the issuer of USDC issuer

Transaction Hashes (Stolen Funds)

- https://etherscan.io/tx/0xaf93a180faa0f90bebb7504febc14413294242e400e77992385a6e207a2d0f56
- https://etherscan.io/tx/0xe4961631af8d731ec66d9784881106e9c636400292ce2ea03c69763fc1bd1d69
- https://tronscan.org/#/transaction/6d4cf01adac2bc12042d9dee234c93c2ff6f8ab68bc990f1c107f5be5d687ad3
- https://tronscan.org/#/transaction/5c7287600d2090002f96368486136a6a17b63ffb0f8c706ab695f2b2691f6e17
- https://www.blockchain.com/explorer/transactions/btc/2f709ae51201b4338544f407053ae5a1e85560bde5abe61a2e6228a456ad0f2a

Movement to CoinEx
Transaction Hash:
0xe5743e475260c093ac31f6a536c867dfc41628e649cd7223c21caaff8c7f0398

☒ WoT N.V. did not give anyone permission to commit this offense.
☒ I hereby file this complaint on behalf of WoT N.V., with the request that the responsible person(s) be criminally prosecuted..
☒ WoT N.V. has suffered financial damages as a result of this incident and therefore joins the case as an injured party (benadeelde partij).
☒ WoT N.V. and I wish to be kept informed about the progress of the investigation.
☒ I hereby hand over the investigation report to you, as included in the attached annex.
☒ I have nothing further to declare..

Nadat de verklaring door de aangever werd doorgelezen, volharde hij hierbij en ondertekende deze met mij, verbalisant.

Aangever,

.....

Kopie aangifte	☒Na ondertekening werd een kopie van de aangifte aan de aangever verstrekt.
Verklaring der tekens	Indien voor een zinsnede een ☐staat, is deze zinsnede slechts van toepassing indien hierin een kruis is geplaatst.

Stolen Cryptocurrency Assets

USDC
- 65,498.50453 USDC
- 1,853.839505 USDC

USDT (converted to USDC)
- 19,438.88959234 USDT
- 333.92 USDT

BTC
- 0.14328483 BTC

Appendix:
- Report of Chainalysis and Crystal Blockchain

- Passport UBO
- Commercial registrations of the companies Wot.NV / G-Force Corporate Services B.V. / Guardian Corporation Curaçao B.V

Sluiting Datum + Plaats	Ik, verbalisant, heb dit proces-verbaal op ambtseed opgemaakt, gesloten en ondertekend op donderdag 26 februari 2026 te Curaçao.
Handtekening verbalisant	